# EXHIBIT A

pplication for a Search Warrant

# UNITED STATES DISTRICT COURT

for the

Northern District of California

| | | |
|---|---|---|
| In the Matter of the Search of<br>*(Briefly describe the property to be searched or identify the person by name and address)*<br>1831 POLK STREET #117, SAN FRANCISCO, CALIFORNIA. | ) | Case No. |

## APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See Attachment A.

located in the Northern District of California, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B incorporated by reference herein

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

| *Code Section* | *Offense Description* |
|---|---|
| See attached Affidavit | See attached Affidavit |

The application is based on these facts:

See Affidavit in Support of Application for Search Warrant

- ☐ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____ ) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Approved as to Form:

AUSA Philip J. Kearney

*Applicant's signature*

SA Michael Eldridge, Federal Bureau of Investigation

*Printed name and title*

Sworn to before me and signed in my presence.

Date: 5-30-14

*Judge's signature*

City and state: San Francisco, California

Jacqueline Scott Corley, U.S. Magistrate Judge

*Printed name and title*

## AFFIDAVIT IN SUPPORT OF APPLICATION FOR SEARCH WARRANT

I, Michael P. Eldridge, hereinafter referred to as affiant, being duly sworn, depose and state as follows:

## INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the residence believed to be occupied by Ryan Kelly Chamberlain II ("CHAMBERLAIN"), which is located at 1831 Polk Street #117, San Francisco, California, 94109 (the "**Subject Premises**"), as is more particularly described in Attachment A, for the items enumerated in Attachment B, which constitute evidence, contraband, fruits, and instrumentalities of violations of Title 18, United States Code, Section 175(a) (production, possession and transfer, or attempted production, possession and transfer, of a biological agent, toxin or delivery system for use as a weapon); and 18 U.S.C. § 175(b) (possession of biological agent, toxin or delivery system not reasonably justified by a prophylactic, protective, bona fide research, or other peaceful purpose)(the "Specified Federal Offenses").

2. I am a Special Agent with the Federal Bureau of Investigation ("FBI"), and have been so employed since July 2013. I am currently assigned to the FBI's San Francisco Division, Oakland Resident Agency ("Oakland RA"). The Oakland RA is tasked with the investigation of federal criminal offenses, including the investigation of weapons of mass destruction ("WMD"), which comprise, in part, biological agents, toxins, explosive devices, and related materials. This application arises from a joint investigation by the FBI, the Bureau of Alcohol, Tobacco, Firearms and Explosives ("ATF"), and the United States Department of Homeland Security, Homeland Security Investigations ("HSI"), of the potential clandestine acquisition and use, and attempted clandestine acquisition and use, of toxins and biological agents by an individual identified as CHAMBERLAIN.

3. I have personally participated in this investigation and am aware of the facts contained herein based on my own investigation, as well as my review of documents, records and information provided to me by other law enforcement officers and technical experts. The other law enforcement officers and experts I have received information from include FBI special agents with training and experience in WMD related investigations. These special agents have received specialized training in WMD investigations and have conducted investigations concerning the production and manufacturing of WMDs, as well as multiple assessments and investigations of the threatened use of WMDs. Based on my personal knowledge, and the information I have received from the law enforcement officers and technical experts described above, I have knowledge, training, and experience regarding the manufacture, deployment, and manufacturing of WMDs. Specifically, I am familiar with biological agents and toxins, including ricin, abrin, and pure nicotine, and their chemical properties, methods of production, how they can be manufactured, as well as their effects on the human body. I have not included every detail or every aspect of my training, education, and experience, but have highlighted those areas most relevant to this application.

4. This affidavit is intended to show that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter. Unless specifically indicated, all conversations and statements described in this affidavit are related in substance and in part. Where I assert that an event took place on a particular date, I am asserting that it took place on or about the date asserted.

5. For the reasons set out in this Affidavit, there is probable cause to believe that one or more of the Specified Federal Offenses have been committed, are being committed, and will continue to be committed by CHAMBERLAIN. Further, there is probable cause to believe that CHAMBERLAIN has utilized the **Subject Premises** to facilitate the commission of one or more

of the Specified Federal Offenses. Moreover, there is probable cause to believe that evidence, contraband, fruits and instrumentalities of violations of the Specified Federal Offenses may be present in the **Subject Premises**.

6. The FBI, ATF, and HSI are jointly investigating the illicit, online sale and purchase of toxins, as well as certain chemicals, materials and equipment related to the manufacture of lethal toxins and controlled substances. As set forth below, the investigation has revealed that CHAMBERLAIN has utilized an anonymous, Internet-based marketplace known as Black Market Reloaded ("BMR") to facilitate the unlawful acquisition and possession of biological agents and lethal toxins from vendors in California and Florida.

## BACKGROUND REGARDING BLACK MARKET RELOADED AND TOR

7. Beginning in or about April 2013, HSI initiated an investigation of illicit sales activity on BMR. The investigation revealed that the BMR website provides a sales platform that enables vendors and buyers who are users of the site to conduct anonymous transactions online involving the sale of a variety of illegal goods, including but not limited to: biological agents, toxins, chemicals, firearms, ammunition, explosives, narcotics, and counterfeit goods.

8. The basic user interface of BMR resembles those of other well-known online marketplaces, such as eBay and Amazon.com. However, unlike mainstream e-commerce websites, BMR is only accessible on the "Tor" network, as further described herein.

9. Every computer device on the Internet has an Internet protocol or "IP" address assigned to it, which is used to route Internet traffic to and from the device. Ordinarily, a device's IP address can be used to determine its physical location and, thereby, its user. The Tor network, however, enables its users to hide their identities, as well as their physical locations.

10. In essence, Tor is a special network of computers on the Internet, distributed around the world, that is designed to conceal the true IP addresses of the computers on the

network and, thereby, the identities of the network's users. Such networks are often referred to as "Darknets," or the "Deepweb."

11. Although Tor has known legitimate uses, it is also known to be used by cybercriminals seeking anonymity in their illicit online activities. Every communication sent through Tor is transferred through numerous relays within the network, and concealed in numerous layers of encryption, such that its users believe it to be virtually impossible to trace communications through Tor back to their true, originating IP addresses.

12. Similarly, Tor enables websites to operate on the network in a way that conceals the true IP addresses of the computer servers hosting the websites, thereby making it extremely difficult to identify the server's physical location. Networks such as Tor are accessible through specialized software that, when installed and configured on a user's personal computer or mobile device, enables the user to access hidden websites, blogs, and other sites and surf the Internet anonymously.

13. Illicit websites operating on Tor have complex web addresses, generated by a computer algorithm, ending in ".onion." Websites with ".onion" addresses can be accessed only by using Tor browser software, which may be downloaded by prospective users from the Internet.

14. At all times relevant to HSI's investigation of this matter, BMR maintained a ".onion" web address on the Tor network.

**The Bitcoin Payment System**

15. The primary form of payment used on the BMR website is a form of digital currency known as Bitcoins. Bitcoins are a decentralized form of electronic currency, existing entirely on the Internet and not in any physical form. The currency is not issued by any government, bank, or company, but rather is generated and controlled automatically through

computer software operating on a "peer to peer" network. Bitcoin transactions are processed collectively by the computers composing the network.

16. While Bitcoins have known legitimate uses, they are also known to be utilized by cyber-criminals given the ease with which they can be used to move money in relative anonymity.

17. Generally, in order to acquire Bitcoins, a user must purchase them from a Bitcoin "exchanger." In return for a commission, Bitcoin exchangers accept payments of currency in some conventional form (cash, wire transfer, etc.), and exchange the money for a corresponding number of Bitcoins, based on a fluctuating exchange rate. Exchangers also accept payments of Bitcoin and exchange the Bitcoins back for conventional currency, again, charging a commission for the service.

18. Once a user acquires Bitcoins from an exchanger, the Bitcoins are kept in a virtual "wallet" associated with a Bitcoin "address," designated by a complex string of letters and numbers. The "address" is analogous to the account number for a bank account, while the "wallet" is analogous to a bank safe where the money in the account is physically located. Once a Bitcoin user funds the user's wallet, the user can then use Bitcoins in the wallet to conduct financial transactions by transferring Bitcoins from the user's Bitcoin address to the Bitcoin address of another user over the Internet.

19. BMR's payment system essentially consists of a Bitcoin "bank" internal to the website, where BMR users must hold an account in order to conduct transactions on the site.

20. In order to post listings on the BMR site, a vendor must first establish a seller's profile. In order to make a purchase on BMR from a vendor on the site, a user must establish an account on BMR, and then transfer the user's Bitcoins to a Bitcoin address associated with the user's BMR account.

21. After funding one's account, the user can then make purchases from BMR vendors. When the user purchases an item on BMR, the Bitcoins needed for the purchase are held in escrow in a virtual wallet maintained by BMR pending completion of the transaction.

22. Alternatively, at their discretion, transactions by and between users and vendors which were initiated on BMR can also be facilitated through other means, including the use of non-BMR based, virtual Bitcoin wallets, pre-paid "moneypaks" such as Green Dot Moneypak[1], as well as by traditional means, including postal money orders, and Western Union money transfers.

## ABRIN, RICIN, AND PURE NICOTINE

23. Abrin, ricin, and pure nicotine are toxins as defined in 18 U.S.C. § 178(2). Abrin and ricin are listed as select agents by the United States Department of Health and Human Services. *See* 42 C.F.R. § 73.3. Select agents and toxins are a subset of biological agents and toxins that the Department of Health and Human Services ("HHS") and Agriculture ("USDA") have determined to have the potential to pose a severe threat to public health and safety, to animal or plant health, or to animal or plant products. Abrin and ricin naturally exist in, and may be extracted from, the seeds of the rosary pea plant (*abrus precatorius*), and the castor bean plant (*ricinus communis*), respectively. The extraction of abrin and ricin from these seeds is relatively easy and does not require technical expertise. Procedures and methods for this extraction are available from open sources on the Internet.

24. Small doses of abrin and ricin are lethal to human beings if ingested, inhaled, or injected. Symptoms from poisoning from abrin and ricin can include difficulty breathing,

[1]The Moneypak enables its user to send cash to a variety of destinations without the use of a bank account. Essentially, once purchased with cash by a user, the user can then anonymously use the Moneypak to replenish existing pre-paid cards offered by companies such as Green Dot, H&R Block, and Rush Card, among others. Additionally, the Moneypak can be used to fund existing PayPal accounts, or to make same-day payments to certain vendors. PayPal, of course, is a well-established, online payment system.

nausea, vomiting, and diarrhea, with possible death occurring within 36 to 72 hours. According to information posted by the Center for Disease Control ("CDC") on its website, there are no known antidotes for poisoning from abrin or ricin.

25. Extracting the abrin and ricin from the seeds of their respective plants may involve the use of milling and grinding equipment. In addition, solvents – including but not limited to acetone, lye, chloroform and diethyl ether – may be used for the extraction. Laboratory glassware is also equipment that is well-suited to the extraction and purification processes involved in the manufacture and production of abrin and ricin.

26. Pure nicotine appears as a colorless to pale yellow, oily liquid that turns brown upon exposure to air or light. It is soluble in water as well as numerous organic solvents. Nicotine is considered a poison by the CDC and can be absorbed through intact skin, in addition to the respiratory and digestive tracts. Pure nicotine is separate and distinct from the type of nicotine ingested recreationally by the smokers of tobacco cigarettes.

27. Your affiant has been informed by subject matter experts at the FBI National Laboratory in Quantico, Virginia, that pure nicotine affects the central and sympathetic nervous systems, and overexposure may result in death from the paralysis of respiratory muscles. Subject matter experts at the FBI National Laboratory further informed your affiant that the toxicity of nicotine depends upon the route of exposure, and that poisoning by nicotine, also known by nicotinism, is characterized by stimulation and subsequent depression of the central and autonomic nervous symptoms resulting in potential respiratory paralysis leading to death.

## PROBABLE CAUSE

28. On February 14, 2014, a resident of New York State, WITNESS 1, brought a vial containing a white powdery substance into the New York City Police Department's ("NYPD") 49th Precinct. In subsequent interviews with NYPD officers and FBI special agents, WITNESS

I admitted to purchasing cyanide and abrin on BMR for the purpose of committing suicide. Preliminary testing of the items recovered from WITNESS 1and his residence confirmed cyanide was detected on items seized during the search. WITNESS 1 told investigators that he destroyed the samples of abrin that were shipped to him along with the cyanide.

29. Investigators determined that the toxins were shipped to WITNESS 1on December 5, 2013, from a United Parcel Service ("UPS") store in Vacaville, California. Records obtained from that UPS Store determined that the same individual who shipped the toxins to WITNESS 1 also shipped a second package on the same day to a "Ryan Kelly" at the **Subject Premises**. On May 9, 2014 your affiant accessed California Department of Motor Vehicles ("DMV") records, and learned that a Ryan Kelly Chamberlain II (CHAMBERLAIN) listed his residence address as the **Subject Premises**. Surveillance teams first observed CHAMBERLAIN entering and exiting the **Subject Premises** on May 19, 2014. The surveillance teams thereafter observed CHAMBERLAIN entering and exiting the **Subject Premises** approximately eighteen times from May 20, 2014 through May 27, 2014. Based on these observations, your affiant believes CHAMBERLAIN resides at the **Subject Premises**. Your affiant further believes that the apparent use by CHAMBERLAIN of just his first and middle names for the described UPS shipment is significant, and indicative of a potential attempt by CHAMBERLAIN to disguise his true identity.

30. As part of the FBI, ATF, and HSI's joint investigation of BMR, investigators were able to correlate WITNESS 1's purchase of the aforementioned biological agents and toxins to a vendor on BMR using an online moniker or alias. This vendor advertised the production, testing, and sale of biological toxins, improvised explosives, and firearms via BMR. Investigators determined the true identity of this vendor to be WITNESS 2, a Sacramento, California resident.

31. FBI agents arrested WITNESS 2 on May 5, 2014 based on a federal complaint alleging four firearms and explosives offenses, including violations of 18 U.S.C. §§ 922(a)(1)(A), 922(o), and 844(o), and one violation of 26 U.S.C. 5861(f).[2] A forensic analysis of items seized from WITNESS 2 and his property following his arrest tested positive for abrin. In subsequent interviews with investigators, WITNESS 2 admitted that he indeed used the online moniker or alias referenced above on BMR to sell biological toxins, improvised explosives, and firearms to purchasers throughout the United States. WITNESS 2 further admitted that he shipped packages to both WITNESS 1 in New York, and "Ryan Kelly" at the **Subject Premises** on December 5, 2013, from the aforementioned UPS Store in Vacaville, California.

32. WITNESS 2 stated he obtained the name "Ryan Kelly" from a San Francisco buyer (hereinafter "SFB") on BMR who responded to one of WITNESS 2's BMR postings for the sale of abrin. After SFB's initial response to WITNESS 2's advertisement, WITNESS 2 and SFB communicated via Bitmail e-mail.[3] SFB indicated to WITNESS 2 that he previously sought to procure liquid ricin from another seller on BMR, but the liquid ricin was too expensive. SFB further indicated that he was seeking abrin to "ease the suffering" of cancer patients. SFB also asked WITNESS 2 questions about abrin, such as dosing size, dose to body weight ratio, time of effect, and whether an autopsy could detect whether abrin had been used to kill an individual. WITNESS 2 recalled SFB stating that the initial purchase of abrin would be a trial run, and if it was successful, SFB would use the abrin on a larger scale.

33. WITNESS 2 and SFB negotiated the sale of samples of abrin at the cost of

[2] Your affiant has been informed by federal law enforcement personnel that WITNESS 2 is currently represented by counsel and has agreed to enter a plea in federal court to a violation of 18 U.S.C. §175(a).

[3]Bitmail e-mail is a secure e-mail service accessed through Tor. In Bitmail, each user has a random string of numbers attributed to their profile. Therefore, the profile name is attributed randomly, and not chosen by the user like a profile name would be by using e-mail services such as Gmail.

$250.00 per sample. WITNESS 2 stated that SFB directed WITNESS 2 to ship the samples to "Ryan Kelly" at the **Subject Premises**.

34. WITNESS 2 stated that due to his concern with SFB's comments about easing the suffering of cancer patients, and unanticipated complications with the synthesis process for abrin, WITNESS 2 did not ship chemically purified abrin to the purchaser. Instead, on December 5, 2013, WITNESS 2 shipped to "Ryan Kelly" at the **Subject Premises** two clear vials, each containing ground rosary peas, which were ground finely enough to become aerosolized. Your affiant confirmed on May 29, 2014 with the Chief of the Scientific Response Unit of the FBI National Laboratory in Quantico, Virginia that the total amount of chemically pure abrin potentially in these vials would be enough to constitute [conservatively] hundreds of lethal doses of the toxin if metabolized in the human body. Your affiant was also informed by the Chief of the Scientific Response Unit of the FBI National Laboratory that ground abrin, similar to the type shipped by WITNESS 2 to CHAMBERLAIN, would suffer little or no degradation over time if properly maintained in a dry state. WITNESS 2 placed the vials in two small Harbor Freight brand flashlights (with battery packs removed),[4] which were in turn placed in a manila envelope with bubble wrap on the inside for protection. WITNESS 2 estimated the total weight of the package was less than one pound.

35. UPS business records obtained by investigators confirmed that WITNESS 2, using an alias, shipped a package weighing 0.20 pounds to Ryan Kelly, at the **Subject Premises**, on December 5, 2013. UPS records further confirmed that the package was delivered to the **Subject Premises** on December 6, 2013.

36. WITNESS 2 related to FBI investigators that sometime after he shipped the abrin

[4] Searches performed by investigators following the arrests of both WITNESS 1and WITNESS 2 resulted in the seizure of multiple small Harbor Freight brand flashlights from both individuals. Investigators also seized receipts showing the purchase of Harbor Freight brand flashlights following the arrest of WITNESS 2.

precursor powder to SFB, SFB contacted WITNESS 2 via Bitmail and complained that the abrin did not work. WITNESS 2 apologized and alluded to sending SFB another shipment of abrin, but SFB ceased communication with WITNESS 2 after that point. WITNESS 2 believed that after they ceased their communication, SFB was still looking to acquire toxins due to his previously failed attempt or attempts.

37. Additional investigation into BMR by FBI and HSI agents led investigators to WITNESS 3, a Florida resident and vendor on BMR. WITNESS 3 utilized an alias on BMR to advertise the sale of items including, but not limited to, ricin, abrin, and psilocybin mushrooms.[5] WITNESS 3 was arrested by the FBI in Florida on January 18, 2014 for offenses including, but not limited to, the production, testing, and sale of biological toxins, including ricin and abrin.

38. A subsequent search of WITNESS 3's laptop computer seized during the search of his residence produced a file containing the names and associated addresses of three individuals, including one for "Ryan Kelly, 1831 Polk Street, San Francisco, California 94109. The search of WITNESS 3's laptop also produced a United States Postal Service ("USPS") Priority Mail label and receipt, addressed to "Ryan Kelly, 1831 Polk Street, Apt 117, San Francisco, CA 94109-3013", (the **Subject Premises**), with a "Ship Date" of June 26, 2013.

39. During a post-arrest interview with FBI investigators, WITNESS 3stated that "Ryan Kelly" was the name of the first person he sold anything to on BMR. WITNESS 3said that "Kelly" initially responded to WITNESS 3's BMR posting for the sale of psilocybin mushrooms, but instead asked WITNESS 3 if WITNESS 3 could make pure nicotine.

40. WITNESS 3 responded that he could do so, and later extracted the nicotine from nicotine patches he already possessed. WITNESS 3 said he made approximately 140 to 200

[5] Psilocybin mushrooms are illegal hallucinogenic Schedule I substances under the Controlled Substances Act. According to that Act, Schedule I drugs, which include heroin and LSD, have a high potential for abuse and serve no legitimate medical purpose in the United States.

milligrams (mg) of pure nicotine (approximately five to ten milliliters in volume), and packaged the material in a small glass vial which he wrapped in bubble wrap. WITNESS 3 then placed the wrapped vial inside a plastic VHS tape case, which he in turn placed in a USPS Priority Mail box. WITNESS 3 shipped the box via the LaBelle, Florida Post Office to "Ryan Kelly" at the **Subject Premises** on June 26, 2013. WITNESS 3 recalled that once the transaction was finalized, "Kelly" left feedback on WITNESS 3's seller page on BMR.

41. Based on your affiant's observations, the observations of other FBI SAs communicated to your affiant, and discussions with employees of the Real Estate Agency that manages the building containing the **Subject Premises**, the **Subject Premises** is a residential apartment in a two story, mixed-use building on the Southwest corner of Polk and Jackson Streets in San Francisco. The mixed-use building containing the **Subject Premises** contains commercial storefronts along the ground floor sidewalks of both Polk and Jackson Streets, with 16 residential apartments above and behind those storefronts. The **Subject Premises**, further described in Attachment A, is a one bedroom residential apartment on the ground floor of 1831 Polk Street. The residential units within 1831 Polk Street are accessible through entry doors located on both Polk and Jackson Streets.

42. On May 27, 2014, your affiant met with an employee of the Real Estate Agency that manages the building containing the **Subject Premises**, who told your affiant that CHAMBERLAIN is the sole listed tenant of the **Subject Premises**, and has been since October 1, 2010.

43. CHAMBERLAIN has two prior felony arrests in the State of California (resulting in dismissals for further investigation and lack of sufficient evidence), including one 2003 arrest for assault with a deadly weapon or force likely to produce great bodily injury and child cruelty, and one 2009 arrest for battery and injury of a child. On May 15, 2014, your affiant accessed

California Employment Development Department ("EDD") records, which indicated that CHAMBERLAIN has no known present employment. Observations made by surveillance teams between May 19, 2014 and May 27, 2014 were consistent with EDD records showing that CHAMBERLAIN has no known present employment.

44. Based on your affiant's training and experience, and based on the investigation outlined above, it is the opinion of your affiant that CHAMBERLAIN actively uses illicit websites to acquire illegal toxins. Given his multiple attempts to acquire such toxins over an extended period, your affiant believes he may potentially be using other illicit websites and/or vendors to acquire such toxins, and receive or store them in the **Subject Premises**. Your affiant further believes that CHAMBERLAIN may have retained a portion of the two abrin vials shipped to him by WITNESS 2 in December 2013, based on the fact that only a small portion of the contents of just one of the vials (if pure abrin), could have been sufficient to kill a human being, and that the toxin in powder form could still retain its lethality to the present date. Your affiant further believes based on the investigation, that once CHAMBERLAIN learned from WITNESS 2 that the initial batch of abrin shipped by WITNESS 2 was defective, CHAMBERLAIN could have completed the refining process of that abrin precursor himself. As noted previously, the process of refining rosary peas into pure abrin can be completed with open source information available on the Internet and a minimum of chemicals and equipment.

45. Based on my training and experience, and on conversations that I have had with other law enforcement officers, I am familiar with the practices and methods of persons who traffic in toxins and their reliance on computer technology to commit these criminal offenses. Such individuals often create and maintain records relating to the conduct, including correspondence and memos, receipts, telephone records, bank account and financial information, notes and personal documents, the names or aliases of vendors and co-conspirators, and records

of on-line research relating to toxins and their use stored in electronic or magnetic form in electronic databases and computers

46. As discussed above, users of Tor must download software on to their personal computer devices which allows them to access Tor. Your affiant believes based on training and experience that such software remains on a user's computer unless specifically removed. Based on information learned during this investigation as described above, your affiant believes that the individual identified as "Ryan Kelly" (believed by your affiant to be CHAMBERLAIN), attempted to acquire bio-toxins on multiple occasions over an extended period lasting at a minimum from June through December of 2013. Given this history, your affiant believes that the device or devices used to access the Tor website by "Ryan Kelly" will still have Tor software downloaded on them, as well as other relevant material further described in Attachment B, that constitutes evidence of a violation or violations of 18 U.S.C. §§ 175(a) and 175(b). Based on this information, and on the facts set forth above, there is probable cause to believe that computer-related equipment containing evidence of the Specified Federal Offenses may be found at the **Subject Premises**.

47. Based on my experience, I am informed and believe that individuals seeking to illegally use biological agents or toxins often keep literature on the subject for both their own education, and to better inform their efforts to use such biological agents or toxins. Such literature can take the form of books, periodicals, articles, handbooks, and press reports, in both hard copy, and electronic format. Your affiant believes that the presence of such literature in the **Subject Premises** would constitute potential evidence of violations of the subject federal offenses.

## SPECIFICS RE SEARCH AND SEIZURE OF COMPUTER SYSTEMS

48. Computer hardware, software, documentation, passwords, and data security

devices may be important to a criminal investigation because the items themselves may be instrumentalities, fruits, and/or evidence of crime (including storing information about crimes in the form of electronic data). Thus, Rule 41 of the Federal Rules of Criminal Procedure permits the government to search and seize computer hardware, software, documentation, passwords, and data security devices which are instrumentalities, fruits and/or evidence of crime (including storage devices containing information and evidence about crimes).

49. Searching and seizing information from computers often requires agents to seize most electronic storage devices (along with related peripherals) to be searched later by a qualified computer expert in a laboratory or other controlled environment. This is true because of the following:

a. Computer storage devices can literally store thousands of images and video files. Additionally, a suspect may try to conceal evidence by storing it with a deceptive file name and in a difficult to find location. This may require searching authorities to examine all of the stored data to determine which particular files are evidence and/or instrumentalities of crime. This sorting process can take weeks or months, depending on the volume of data stored, and often it would be impractical to attempt this kind of search on site.

b. Searching computer systems for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment. For example, on site and laboratory analysis by a qualified computer specialist is often required in order to properly retrieve and analyze electronically stored (computer) data, document and authenticate the data, and prevent the loss of the data either from accidental or deliberate programmed destruction.

c. In many cases, the evidentiary data can be backed up to government owned computer data storage devices at the site of the search. However, there are circumstances that may necessitate the seizure and removal of the entire computer system and peripheral devices to

a secure laboratory setting in order to analyze and extract the evidence.

d. To effect accurate and complete analysis may require seizure of all computer equipment and peripherals which may be interdependent, the software to operate the computer system, data security devices (including passwords) and related instruction manuals which contain directions concerning the operation of the computer system and software programs. This is true because the peripheral devices which allow users to enter or retrieve data from the storage devices vary widely in their compatibility with other hardware and software.

e. Many system storage devices require particular input/output devices in order to read the data on the system. It is important that the computer expert be able to properly re-configure the system as it now operates in order to accurately retrieve the evidence.

f. In addition, the computer expert needs the relevant system software (operating systems, interfaces, and hardware drivers) and any applications software which may have been used to create the data (whether stored on hard drives or on external media), as well as all related instruction manuals or other documentation and data security devices.

50. The terms "records," "documents," and "materials" include all of the items described in Attachment B in whatever form and by whatever means they may have been created and/or stored. This includes any handmade, photographic, mechanical, electrical, electronic, and/or magnetic forms. It also includes items in the form of computer hardware, software, documentation, passwords, and/or data security devices as further described below:

a. Computer Hardware. Computer hardware consists of all equipment which can collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, optical, or similar computer impulses or data. This includes any data-processing devices (such as central processing units, memory typewriters, and self-contained "laptop" or "notebook" computers, tablets, and smart phones); internal and peripheral storage devices (such as fixed

disks, external hard disks, floppy disk drives and diskettes, tape drives and tapes, optical storage devices, transistor-like binary devices, compact flash cards, USB flash drives, smart media cards, and other memory storage devices); peripheral input/output devices (such as keyboards, printers, scanners, plotters, video display monitors, televisions utilized as monitors, and optical readers); related communications devices (such as modems, cables and connections, recording equipment, RAM or ROM units, acoustic couplers, automatic dialers, speed dialers, programmable telephone dialing or signaling devices, and electronic tone-generating devices); as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (such as physical keys and locks).

b. Computer Software. Computer software is digital information which can be interpreted by a computer and any of its related components to direct the way it works. Software is stored in electronic, magnetic, optical, or other digital form. It commonly includes programs to run operating systems, applications (like word-processing, graphics, or spreadsheet programs), utilities, compilers, interpreters, and communications programs.

c. Computer-related Documentation. Computer-related documentation consists of written, recorded, printed, or electronically stored material which explains or illustrates how to configure or use computer hardware, software, or other related items.

d. Computer Passwords and Other Data Security Devices. Computer passwords and other data security devices are designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates as a sort of digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software or digital code may include programming code that creates "test" keys or "hot" keys, which perform certain pre-set security

functions when touched. Data security software or code may also encrypt, compress, hide, or "booby-trap" protected data to make it inaccessible or unusable, as well as reverse the process to restore it.

51. Based on the above facts and circumstances and information, your affiant requests permission to seize all computer systems and peripherals in the Subject Premises, if necessary even though there may be unrelated information stored on the computer system(s). This unrelated data will not be used and will be separated (to the extent possible) from the evidentiary data described in Attachment B, and preserved as is further discussed in the computer search protocol described in Exhibit C.

## REQUEST FOR SEALING ORDER

52. It is further respectfully requested that this Court issue an Order sealing, until further order of this Court, all papers submitted in support of this application, including the application, affidavit, and search warrant, and attachments thereof. Sealing is necessary because the items and information to be seized are relevant to an ongoing investigation and premature disclosure of the contents of this affidavit and related documents may have a negative impact on this continuing investigation and may jeopardize its effectiveness.

## CONCLUSION

53. Based upon the foregoing, I respectfully request that this Court issue a search warrant for the **Subject Premises** more particularly described in Attachment A, authorizing the

///

///

///

///

///

seizure of the items described in Attachment B, and where appropriate, using the search protocol described in Attachment C.

Under penalty of perjury, I swear that the foregoing is true and correct to the best of my knowledge, information and belief.

Michael P. Eldridge
Special Agent
Federal Bureau of Investigation

Subscribed to and sworn before me on this 30 day of May, 2014.

HONORABLE JACQUELINE SCOTT CORLEY
UNITED STATES MAGISTRATE JUDGE

## ATTACHMENT A

## DESCRIPTION OF LOCATION TO BE SEARCHED

1. The residence previously referred to as the **Subject Premises**, located at 1831 Polk Street #117, San Francisco, California, 94109. The **Subject Premises** is located within a larger building on the West side of Polk Street, South of Jackson Street in San Francisco, California. The larger building housing the **Subject Premises** occupies the Southwest corner of the intersection of Polk and Jackson Streets in San Francisco.

2. The **Subject Premises** is a single, one bedroom apartment unit on the ground floor, located on the West side of the building adjacent to a courtyard at the rear (West side) of the building. The **Subject Premises** has a front door that is green and tan in color and is labeled with the numbers "117." The larger building housing the **Subject Premises** is a two story structure containing both commercial businesses occupying the ground floor along Polk Street, and sixteen residential units on both the ground and upper floors. The **Subject Premises** is the only residential unit on the ground floor. The exterior of the building is tan in color with green trim and a flat roof. Access to the residential units within the building housing the **Subject Premises** is through a front door located on the East side of the building on Polk Street. This front door is green in color, with the numbers "1831" mounted on the top-center of the door. A second or alternative door allowing access to the residential units within the building housing the **Subject Premises** is located on Jackson Street, just west of the intersection of Polk and Jackson Streets. This door is green in color, with the numbers "1609" mounted on the lower left-hand side of the door.

3. The **Subject Premises** to be searched includes the bedroom, bathroom, kitchen, interior rooms, closets, crawl spaces, containers, the Unit 117 mailbox, the Unit 117 storage area

or areas, and Unit 117 trash containers, which may contain any of the items of evidence described in Attachment B.

## ATTACHMENT B

## DESCRIPTION OF ITEMS TO BE SEIZED

Items constituting evidence, contraband, fruits or instrumentalities of violations of 18 U.S.C §§ 175(a) and 175(b), as follows:

1. Records, communications, or other documents, in any form, that demonstrate occupancy, residency, and control of the **Subject Premises** located at 1831 Polk Street #117, San Francisco, California 94109 (further described in Attachment A), including, but not limited to, utility bills, cable bills, telephone bills, toll records, bank account documents, property tax bills and notices, vehicle sales invoices, vehicle titles, and vehicle related documents, as well as property lease documents, titles, and deeds.

2. Records, communications, documents, or objects, in any form, pertaining to postal and private package delivery service to the **Subject Premises**, including but not limited to air bills, receipts, envelopes, mailing labels, postage, packages, and containers.

3. Biological agents, toxins, or delivery systems designed to use biological agents or toxins as weapons, including but not limited to abrin, rosary peas, rosary pea plants (*abrus precatorius*), and pure nicotine.

4. Any tools, devices, implements, storage containers, bags, safety equipment, or items used to produce, store, handle or transport biological agents, toxins, or delivery systems designed to use biological agents or toxins as weapons; and any such items (including sink traps and drains) that contain residue of any biological agents or toxins or delivery systems designed to use biological agents or delivery systems, including but not limited to abrin, rosary peas, rosary pea plants (*abrus precatorius*), and pure nicotine.

5. Records, documents, programs, applications, research, or materials, in any form, relating to the use, acquisition, or storage of biological agents, toxins, or delivery systems

designed to use biological agents or toxins as weapons, including but not limited to abrin, rosary peas, rosary pea plants (*abrus precatorius*), and pure nicotine.

6. Records, documents, programs, applications, research, or material, in any form, relating to attempts to acquire biological agents, toxins, or delivery systems designed to use biological agents or toxins as weapons through the Internet, including but not limited to evidence of the use of the Tor network, the hidden services website Black Market Reloaded (BMR), other related hidden services websites such as Silk Road, Bitmail, or Bitcoin payment websites and/or systems.

7. Records, documents, programs, applications, research, or material, in any form, relating to attempts to communicate or communications with or about the following: individuals identified in the Affidavit of FBI SA Michael P. Eldridge as WITNESS 1, WITNESS 2, AND WITNESS 3, and their respective on-line aliases.

8. With respect to any digital device containing evidence falling within the scope of the foregoing search categories, records, documents, programs, applications, materials, or evidence of the absence or deletion of the same, sufficient to show the actual user(s) of the digital device.

9. With respect to any computer equipment or other electronic devices:

a. Passwords, encryption keys, and other access devices that may be necessary to access the computer equipment;

b. Documents or other items demonstrating the presence or absence of computer software that would allow others to control the items, and presence or absence of security software designed to detect such malicious software;

c. Documents or other items demonstrating the attachment of other computer hardware or storage media;

d. Counter forensic programs and associated data that are designed to eliminate data.

10. As used above, the term "digital device" includes any electronic system or device capable of storing and/or processing data in digital form, including: central processing units; laptop or notebook computers; personal digital assistants; wireless communication devices such as telephone paging devices, beepers, and mobile telephones; peripheral input/output devices such as keyboards, printers, scanners, plotters, monitors, and drives intended for removable media; related communications devices such as modems, cables, and connections; storage media such as hard disk drives, floppy disks, compact disks, magnetic tapes used to store digital data (excluding analog tapes such as VHS), and memory chips; and security devices. Such digital devices will be searched pursuant to the protocol described in Attachment C.

## ATTACHMENT C

## THE NORTHERN DISTRICT OF CALIFORNIA PROTOCOL FOR SEARCHING DEVICES OR MEDIA THAT STORE DATA ELECTRONICALLY

1. In executing this warrant, the government will begin by ascertaining whether all or part of a search of a device or media that stores data electronically ("the device") reasonably can be completed at the location listed in the warrant ("the site") within a reasonable time. If the search reasonably can be completed on site, the government will remove the device from the site only if removal is necessary to preserve evidence, or if the item is contraband, a forfeitable instrumentality of the crime, or the fruit of a crime.

2. If the government determines that a search reasonably cannot be completed on site within a reasonable time period, the government must determine whether all or part of the authorized search can be completed by making a mirror image of, or in some other manner duplicating, the contents of the device and then conducting the forensic review of the mirror image or duplication off site. The government will complete a forensic review of that mirror image within 120 days of the execution of the search warrant.

3. In a circumstance where the government determines that a mirror image of the contents of a device cannot be created on site in a reasonable time, the government may seize and retain that device for 60 days in order to make a mirror image of the contents of the device.

4. When the government removes a device from the searched premises it may also remove any equipment or documents ("related equipment or documents") that reasonably appear to be necessary to create a mirror image of the contents of the device or conduct an off-site forensic review of a device.

5. When the government removes a device or related equipment or documents from the site in order to create a mirror image of the device's contents or to conduct an off-site forensic review of the device, the government must file a return with a magistrate judge that identifies with particularity the removed device or related equipment or documents within 14 calendar days of the execution of the search warrant.

6. Within a reasonable period of time, but not to exceed 60 calendar days after completing the forensic review of the device or image, the government must use reasonable efforts to return, delete, or destroy any data outside the scope of the warrant unless the government is otherwise permitted by law to retain such data.

7. The time periods set forth in this protocol may be extended by court order for good cause.

8. In the forensic review of any device or image under this warrant the government must make reasonable efforts to use methods and procedures that will locate and expose those categories of files, documents, or other electronically-stored information that are identified with particularity in the warrant, while minimizing exposure or examination of irrelevant, privileged, or confidential files, to the extent reasonably practicable.

9. For the purposes of this search protocol, the phrase "to preserve evidence" is meant to encompass reasonable measures to ensure the integrity of information responsive to the warrant and the methods used to locate same.